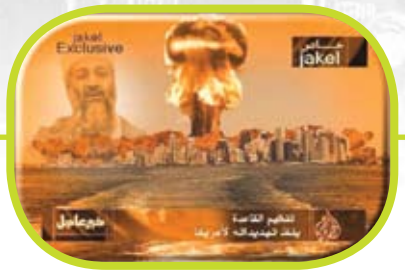
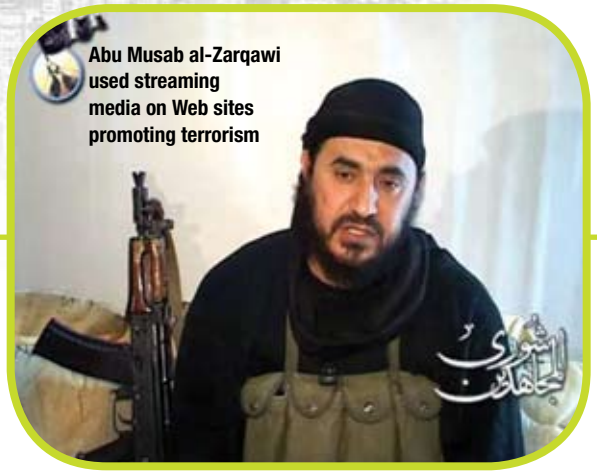
FEATURE

Terrorist Use of the Internet
The Real Story

By IRVING LACHOW
and COURTNEY RICHARDSON



Web site showing nuclear attack on large city



Abu Musab al-Zarqawi used streaming media on Web sites promoting terrorism

terrorist organizations can now affordably duplicate many capabilities needed by modern militaries, governmental organizations, and businesses

Cyberterrorism conjures images of infrastructure failures, economic disasters, and even large-scale loss of life. It also receives a great deal of coverage in the press. While the threat of cyberterrorism is real, the hype surrounding the issue often outpaces the magnitude of the threat. In addition, the term itself deflects attention from a more mundane but equally serious problem: terrorist organizations effectively using the Internet to stymie U.S. efforts to win the Long War.

The Internet enables terrorist groups to operate as either highly decentralized franchises or freelancers. Similar to information age businesses, these groups use the Internet to create a brand image, market themselves, recruit followers, raise capital, identify partners and suppliers, provide training materials, and even manage operations. As a result, these groups have become more numerous, agile, and well coordinated, all of which make them harder to stop.[1] Furthermore, these groups have become expert at using the Internet to manipulate both public opinion and media coverage in ways that undermine American interests. In short, rather than *attacking* the Internet, terrorists are *using* it to survive and thrive.

This article examines why the Internet is so useful for terrorist organizations. It then considers how terrorists use the Internet for strategic advantage and why the threat of cyberterrorism may be overstated in many cases. The article concludes with a set of observations and recommendations.

Why the Internet?

The Internet has five characteristics that make it an ideal tool for terrorist organizations. First, it enables rapid communications. People can hold conversations in real time using instant messaging or Web forums. Instructions, intelligence information, and even funds can be sent and received in seconds via email. Second, Internet use is a low-cost proposition. Terrorist organizations can now affordably duplicate many of the capabilities needed by modern militaries, governmental organizations, and businesses: a communications infrastructure, intelligence-gathering operation, training system, and media-savvy public affairs presence. Third, the ubiquity of the Internet means that small terrorist groups can have a global cyber presence that rivals that of much larger organizations. Terrorists not only can communicate with each other from almost anywhere in the world, but they also can create a Web site that is viewed by millions and possibly even examined daily by media outlets for news stories. Fourth, the growth in bandwidth combined with development of new software has enabled unsophisticated users to develop and disseminate complex information via the Internet. For example, in December 2004, "a militant Islamic chat room posted a twenty-six-minute video clip with instructions on how to assemble a suicide bomb vest, along with a taped demonstration of its use on a model of a bus filled with passengers."[2] Finally, modern encryption technologies allow Internet users to surf the Web, transfer funds, and communicate anonymously—a serious (though not insurmountable) impediment to intelligence and law enforcement organizations trying to find, track, and catch terrorists. To achieve anonymity, terrorists can download various types of easy-to-use computer security software (some of which is commercial and

Dr. Irving Lachow is a Senior Research Professor in the Information Resources Management College at the National Defense University (NDU). Courtney Richardson is a Research Associate in the Center for Technology and National Security Policy at NDU.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Terrorist Use of the Internet: The Real Story	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Institute for National Strategic Studies,260 5th Avenue SW Fort Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

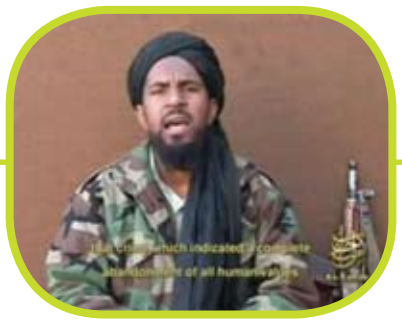
15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**4**	

some of which is freely available) or register for anonymous email accounts from providers such as Yahoo! or Hotmail.

Internet as Strategic Tool

The combination of characteristics described above makes the Internet a valued strategic asset for terrorists. In fact, one could argue that the Internet, along with other modern communications technologies, is a sine qua non of the modern global extremist movements. Successful terrorism requires the transformation of interested outsiders into dedicated insiders.[3] Once someone has become an insider, less intense but still continuous interactions are required to maintain the needed level of commitment to the cause.



Subtitle on militant Web site stating "the crime which indicated a complete abandonment of human values"

Before the advent of advanced communications technologies, this process was entirely based on face-to-face interactions, which limited the scope of a given group. However, the Internet allows groups to create and identify dedicated insiders—and to maintain fervor in those already dedicated to the cause—on a global scale.[4] Advanced technologies also allow the extremists to deliver well-coordinated propaganda campaigns that increase the levels of support among the general public, which in turn allows terrorists to operate freely in these societies. For example, one of al Qaeda's goals is to use the Internet to create "resistance blockades" in order to prevent Western ideas from "further corrupting Islamic institutions, organizations, and ideas."[5] One technique they use is to distribute Internet browsers that have been designed to filter out content from undesirable sources (for example, Western media) without the users' knowledge.[6]

In summary, the development and proliferation of the Internet have enabled the rise of loose, decentralized networks of terrorists all working toward a common goal. In the words of one expert, "it is the strategic—not operational—objectives of the *jihadi* movement's use of technology that engenders the most enduring and lethal threat to the United States over the long term."[7]

Cyberterrorism?

It is evident that terrorist groups are extremely effective in using the Internet to further their missions. Are they also using, or planning to use, the Internet to launch a major cyber attack on the United States? We do not know, but there are a number of factors that suggest the answer to this question is no. Terrorism, by definition, is focused on obtaining desired political or social outcomes through the use of tactics that instill fear and horror in target populations. *Cyberterror* can be defined as:

a computer based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. The attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples. . . . Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[8]

Islamic Web site

History shows that the vast majority of cyber attacks, even viruses that cause billions of dollars of damage to an economy, are not going to cause the levels of fear desired by most terrorists. In comparison, using physical means to create terror is fairly easy and quite effective. Put in these terms, it is not surprising that terrorists prefer to inflict damage with physical means and then use the Internet to magnify the results of their handiwork. Indeed, while there is clear evidence that terrorists have used the Internet to gather intelligence and coordinate efforts to launch physical attacks against various infrastructure targets, there has not been a single documented incidence of cyberterrorism against the U.S. Government.[9]

One could argue that terrorists would use the Internet to attack cyber assets that control physical systems, thereby creating horrific physical effects via cyber means. The most likely scenario of this type is an attack on the control systems that manage parts of the Nation's infrastructure (for example, dams, trains, and powerplants). The consequences of an attack of this kind would be serious, so this threat deserves attention. However, the actual *likelihood* of such an attack is unknown; different analyses have reached different conclusions.[10]

Two things are certain: successfully launching such an attack would not be easy, and the consequences are difficult to predict due to the incredible complexity and interdependence of critical infrastructures. Given a choice of conducting either a cyber attack whose consequences are unknown (and which may not have the desired effect even if it does work) or a physical attack that is almost certain to cause graphic deaths that will create fear, it is understandable why terrorists have (so far) chosen the latter.

Observations

Terrorists use the Internet to harm U.S. national security, but *not* by attacking infrastructure or military assets directly. Instead, terrorists use the Internet to improve their operational effectiveness while simultaneously undermining our military and diplomatic efforts to win the war of ideas. There is little doubt that they are doing both things well. While there is a possibility that they may use the Internet to launch a cyberterror attack against American targets, this threat falls under the broad umbrella of critical infrastructure protection—a topic that is getting a great deal of attention at all levels of government.[11] This issue is not addressed here. Rather, the focus rests on the other two uses of the Internet—issues that are equally important but often receive comparatively less focus, energy, and resources.

Terrorist Operational Effectiveness. The Internet enables terrorist organizations to operate as virtual transnational organizations. They can use it to raise funds, recruit, train, command and control, gather intelligence, and share information. Clearly, it is in the U.S. interest to either disrupt or undermine these activities. The good news is that relying on the Internet is a double-edged sword for terrorist organizations: despite the many benefits associated with using the Internet as their main intelligence, command

and control, and communications system, this approach carries a few liabilities. Terrorist reliance on Web sites and discussion forums allows outsiders to monitor their methods and track trends. For example, there are groups such as the SITE Institute that focus on monitoring terrorist Web sites and providing information to a wide range of interested parties, including elements within the U.S. Government.[12] Reliance on the Internet also creates the opportunity for outsiders to pose as insiders in order to provide misinformation or simply to create doubt among the terrorists about whom they can trust.

To that end, the United States should make every effort to infiltrate extremist virtual communities in order to gather intelligence and begin planting the seeds of mistrust that can disable terrorist cells. We presume that governmental activities of this kind are under way. Surprisingly, nongovernmental organizations appear to contribute to these efforts as well. For example, individual citizens have infiltrated terrorist networks via chat rooms and then worked with governmental agencies to bring about several arrests.[13]

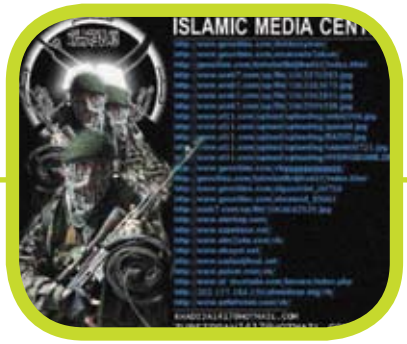
Fatah commander in Lebanon with ties to al Qaeda using Internet

The bad news is that terrorists are doing their best to minimize the liabilities associated with heavy reliance on the Internet. They are quick to learn from mistakes and to disseminate best practices on how to defeat the tactics used by intelligence and law enforcement agencies.[14] Terrorist groups are adept at quickly moving their Web sites from host to host, which makes them difficult to track and shut down (trusted members of these groups use chat rooms, email, and other forums to share information about the new location of a moved site). They also like to masquerade some activities as legitimate business operations.

Terrorist Influence Operations. One of the most difficult challenges facing the United States is countering terrorist use of the Internet to propagate their ideological agenda. This problem is part of the much broader war of ideas against the extremist Islamic movement. Efforts to date have not proven successful, as evidenced by the following statement from former Secretary of Defense Donald Rumsfeld: "If I were grading I would say we probably deserve a 'D' or a 'D-plus' as a country as to how well we're doing in the battle of ideas that's taking place in the world today."[15] This is a complex issue that does not lend itself to easy answers.

Recommendations

U.S. efforts to influence must be tied to real-world actions. While it is easy to focus on the principles of effective communications strategies, our words will ring hollow if they are not related to the realities experienced by the target audience. Thus, it goes without saying that what the United States *does* is as important, if not more so, as what it *says*. To that end, diplomatic and military influence operations must ensure that target audiences are aware of the positive actions undertaken by the United States in the Muslim world, while simultaneously highlighting the negative actions of our enemies.



Islamic Media Center Web site listing Web sites promoting terrorism

The corollary to this point is that the United States must effectively get its story out before the terrorists or insurgents can use the Internet to spin events in their favor. It is much harder to respond to or discredit initial stories, even ones that are untrue, than to establish the baseline facts or perceptions in the first place. There are certainly elements of the U.S. Government making heroic efforts in this area. For example, the Department of State maintains a Web site in a number of languages (including Arabic, Farsi, and French) that is devoted to countering false stories that appear in extremist sources. It also focuses on countering disinformation likely to end up in the mainstream media. U.S. Embassies have used this resource to counter disinformation in extremist print publications in Pakistan and elsewhere. There are also military units deployed overseas that are exhibiting best practices in operational level influence operations.[16] Unfortunately, much work remains to be done for such examples to become the rule rather than the exception.

A related point is that the Nation must view the war of ideas as equal in importance to the military and law enforcement aspects of the war on terror. The war-of-ideas aspect of any decision involving the Long War must be considered at the highest levels of U.S. policymaking. That emphasis must then be communicated down the chain so that all players understand the importance of *message* in this war. Strategic communications cannot be seen as an afterthought of a military operation or as the sole responsibility of an office buried within the State Department. The recent announcement that the Office of the Secretary of Defense is creating a new office focused on strategic communications is a move in the right direction. Similarly, information operations cannot be viewed simply as a set of activities done by a local commander in support of tactical objectives. It is clear from past experience that such approaches are not effective in the long run if they are not tied to strategic considerations.

Countering terrorist use of the Internet to further ideological agendas will require a strategic, government-wide (interagency) approach to designing and implementing policies to win the war of ideas. For example, to counter terrorist influence operations, all Federal agencies should use the same specific and accurate language when referring to Salafist extremists. It is of the utmost importance that American policymakers set their terms of the debate. Expressions such as *jihad* and *mujahideen* are part of the popular lexicon describing antiterrorist operations in Iraq, Afghanistan, and elsewhere. However, such terms disempower the United States. Jihad literally means "striving" and is frequently used to describe every Muslim's responsibility to strive in the path of God. Mujahideen is closely translated to mean "holy warriors." Such a term may have worked to U.S. advantage in Afghanistan against the Soviet Union—however, terms such as these now pit the United States as the enemy against holy warriors in a holy war. Rather, terms such as *hirabah* ("unholy war") and *irhabists* ("terrorists") should become part of the popular lexicon.[17]

As important as it is for the United States to improve its own communications efforts, a key part of countering extremist misinformation and propaganda is to have messages come from a variety of sources—preferably some of them local. For example, it is critical for the United States to promote the views of well-respected Muslim clerics, who counter the claims made by Islamic terrorists and extremists. Such efforts have been undertaken by the government of Saudi Arabia, but American efforts in this area have been lacking.[18] In effect, the Nation should do everything possible to enable moderate Muslims to develop a strong, vibrant, and responsive Internet and media presence of their own.

Internet café

Last but not least, resources must be made available to support all of these efforts, plus others that are not mentioned here but are equally important, such as training and education to improve understanding of Muslim cultures and languages spoken within these cultures. Current U.S. resources dedicated to strategic communications, public diplomacy, and information operations are woefully inadequate.[19] On the military side, the lack of training and education in information operations at all levels—strategic, operational, and tactical—often requires commanders to learn on the job and build information operations teams "out of hide."[20] While some leaders will certainly rise to the occasion, this approach is not a recipe for success in a complex, media-heavy war against adversaries who are highly adept at conducting their own influence operations.

Terrorists use the Internet to harm U.S. national security interests, but not by conducting large-scale cyber attacks. Instead, they use the Internet to boost their relative power to plan and conduct physical attacks, spread their ideology, manipulate the public and media, recruit and train new terrorists, raise funds, gather information on potential targets, and control operations. If these activities can be curtailed, then the viability of the terrorist groups themselves may be put into question. To that end, the United States needs to focus more resources into two areas: countering the operational effectiveness associated with terrorist use of the Internet, and undermining Internet-based terrorist influence operations. If it can successfully meet these two challenges, the United States will make significant progress toward winning the Long War. **JFQ**

NOTES

[1] See Statement of Henry A. Crumpton, Coordinator for Counterterrorism, Department of State, Committee on Senate Foreign Relations, June 13, 2006.

[2] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: U.S. Institute of Peace, 2006), 126–127.

[3] This process, and the impact of the Internet upon it, are described in Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004), 158–161.

[4] The recruiting process is usually not entirely done in cyberspace. At some point, face-to-face meetings are used to assess the level of commitment of potential members. See Sageman, 163.

[5] Jarret M. Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," *The Fletcher Forum of World Affairs* 30, no. 2 (Summer 2006), 160.

[6] Matthew Kovner, "Jihadist Web Browser," Terror Web Watch, Terrorism Research Center, February 3, 2006, available at <www.trc.com>. See also Brachman, 152.

[7] Brachman, 150. Emphasis in original.

[8] Dorothy E. Denning, "Is Cyber Terror Next?" in *Understanding September 11*, ed. Craig Calhoun, Paul Price, and Ashley Timmer (New York: The New Press, 2002), 193.

[9] Evidence of the former is cited in Stephen Ulph, "Internet Mujahideen Intensify Research on U.S. Economic Targets," *Terrorism Focus* 3, no. 2 (January 18, 2006). The latter observation comes from several sources, including Weimann, 149; and Joshua Green, "The Myth of Cyber-Terrorism," *Washington Monthly*, November 2002, available at <www.washingtonmonthly.com/features/2001/0211.green.html>.

[10] For differing perspectives on this issue, see James Lewis, "Cyber Terror: Missing in Action," *Knowledge, Technology & Policy* 16, no. 2 (Summer 2003), 34–41; and Dan Verton, *Black-Ice: The Invisible Threat of Cyber-Terrorism* (New York: McGraw-Hill/Osborne, 2003).

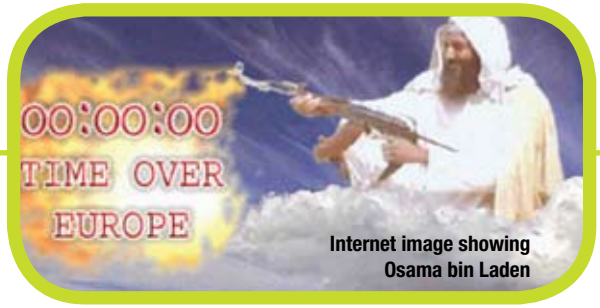
[11] See, for example, The White House, *The National Strategy to Secure Cyberspace*, February 2003; and Department of Homeland Security, *National Infrastructure Protection Plan*, 2006.

[12] See Benjamin Wallace-Wells, "Private Jihad," *The New Yorker*, May 29, 2006.

[13] For example, see Blaine Harden, "In Montana, Casting a Web for Terrorists," *The Washington Post*, June 4, 2006, A3.

[14] For example, see Abdul Hameed Bakier, "The Evolution of Jihadi Electronic Counter-Measures," *Terrorism Monitor* 4, no. 17 (September 8, 2006).

[15] See <www.cbsnews.com/stories/2006/03/27/terror/main1442811.shtml>.



Internet image showing Osama bin Laden

[16] An excellent example is found in Colonel Ralph O. Baker, USA, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations," *Military Review* (May-June 2006), 13–32. This article should be required reading for everyone in the U.S. Government remotely involved in the Long War, and especially for Active duty forces heading to Iraq and Afghanistan.

[17] For more detail, see Douglas E. Streusand and Harry C. Tunnell, "Choosing Words Carefully: Language to Help Fight Islamic Terrorism," Center for Strategic Communications, National Defense University, available at <www.ndu.edu/csc/products.cfm>; and Jim Guirard, "Hirabah versus Jihad: Rescuing Jihad from the al Qaeda Blasphemy," *The American Muslim*, July 6, 2003, available at <http://theamericanmuslim.org/tam.php/features/articles/terrorism_hirabah_versus_jihad_rescuing_jihad_from_the_al_qaeda_blasphemy/>.

[18] For more details, see Robert Spencer, "Losing the War of Ideas," FrontPageMagazine.com, February 5, 2004.

[19] See, for example, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Report of the Defense Science Board Task Force on Strategic Communication* (Washington, DC: Department of Defense, September 2004).

[20] Baker, 20.

FEATURE